

CRYPTO-GRAM
15 aprile 2009

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA
<<http://www.communicationvalley.it/>>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:
<<http://www.schneier.com/crypto-gram-0703.html>>.

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier "Schneier on Security": <<http://www.schneier.com/blog>>.

Crypto-Gram è anche consultabile in formato RSS.

** *** ***** ***** ***** ***** ***** ***** *****

In questo numero:

- Quarta edizione del concorso "Minaccia da Trama Cinematografica"
- Chi dovrebbe occuparsi della sicurezza cibernetica degli Stati Uniti?
- News
- La privacy e il Quarto Emendamento
- Le news su Schneier
- La definizione di "Armi di distruzione di massa"
- I furti di materiali di prima necessità
- Commenti dei lettori

** *** ***** ***** ***** ***** ***** ***** *****

Quarta edizione del concorso "Minaccia da Trama Cinematografica"

Diciamoci la verità, la Guerra al Terrore è un marchio ormai stanco. Non c'è abbastanza azione nel mondo per terrorizzare la gente. Se questa tendenza continua così, il pubblico si dimenticherà di spaventarsi. E a quel punto sia i terroristi, sia il complesso industriale del terrore perderanno. Non possiamo permetterlo.

Daremo il nostro contributo per ravvivare il terrore. Esistono molte cose di cui aver paura, se solo il pubblico le considerasse secondo la giusta prospettiva. In questa Quarta edizione del concorso "Minaccia da Trama Cinematografica" l'obiettivo è trovare un evento realmente accaduto da qualche parte nel mondo industrializzato (pescare fra

gli eventi del Terzo Mondo è troppo facile) e fornire una teoria complottista che dimostri come i veri responsabili dietro quell'evento furono i terroristi.

Che il vostro contributo sia assurdo ma plausibile, improbabile ma possibile, e -- se solo fosse vero -- terrificante. I contributi dovranno avere il formato di notizie di cronaca e il limite sarà di 150 parole (stavolta controllerò personalmente) perché occorre instillare la paura in una popolazione con una durata di attenzione molto ridotta. I contributi dovranno essere inviati come commenti al post sul blog entro la fine del mese.

Inviare il proprio contributo qui:

<http://www.schneier.com/blog/archives/2009/04/fourth_annual_m.html>

Un esempio da The Onion:

<<http://www.theonion.com/content/cartoon/feb-23-2009>>

La Prima edizione del concorso "Minaccia da Trama Cinematografica":

<http://www.schneier.com/blog/archives/2006/04/announcing_movi.html>

<http://www.schneier.com/blog/archives/2006/06/movieplot_threa_1.html>

La Seconda edizione del concorso "Minaccia da Trama Cinematografica":

<http://www.schneier.com/blog/archives/2007/04/announcing_seco.html>

<http://www.schneier.com/blog/archives/2007/06/second_annual_m.html>

<http://www.schneier.com/blog/archives/2007/06/second_movieplo.html>

La Terza edizione del concorso "Minaccia da Trama Cinematografica":

<http://www.schneier.com/blog/archives/2008/04/third_annual_mo.html>

<http://www.schneier.com/blog/archives/2008/05/third_annual_mo_2.html>

<http://www.schneier.com/blog/archives/2008/05/third_annual_mo_1.html>

** *** ***** ***** ***** ***** ***** ***** *****

Chi dovrebbe occuparsi della sicurezza cibernetica degli Stati Uniti?

La sicurezza cibernetica del governo degli Stati Uniti è un gran pasticcio di insicurezza, e per cercare di risolverlo sarà necessario investire una considerevole quantità di risorse e di lavoro. Nel tentativo di avere un quadro generale della situazione, il presidente Barack Obama ha ordinato una revisione di 60 giorni delle iniziative di sicurezza cibernetica governativa. Nel frattempo lo U.S. House Subcommittee on Emerging Threats, Cybersecurity, Science and Technology sta tenendo delle udienze sul medesimo argomento.

Uno degli argomenti motivo di disputa è chi dovrebbe essere responsabile della sicurezza cibernetica. L'FBI, il Dipartimento per la Sicurezza Nazionale e il Dipartimento della Difesa (la NSA nello specifico) hanno ognuno i propri interessi in quest'ambito. Poche settimane fa Rod Beckstrom ha dato le dimissioni dal suo incarico in qualità di direttore del National Cybersecurity Center del Dipartimento per la Sicurezza Nazionale, mettendo in guardia di una possibile presa di potere da parte della NSA.

Mettere la sicurezza cibernetica nazionale nelle mani della TSA è un'idea incredibilmente pessima. Un gran numero di figure, da Louis Freeh (ex-direttore

dell'FBI) a Scott Charney (vicepresidente del Trusted Computing Group di Microsoft nonché ex-direttore della sezione reati informatici del Dipartimento di Giustizia) hanno manifestato la stessa opinione al Congresso durante le udienze di questo mese.

La sicurezza cibernetica non è un problema dell'esercito, e nemmeno un problema del governo -- è un problema universale. Tutte le reti, militari, governative, civili e commerciali, si servono degli stessi computer, del medesimo hardware di rete, dei medesimi protocolli Internet e degli stessi pacchetti software. Tutti siamo nel mirino degli stessi strumenti e tattiche di attacco. E non si può nemmeno dire che i bersagli governativi siano in qualche modo più importanti; attualmente la maggior parte dell'infrastruttura IT critica del nostro paese è in mani commerciali. E hacker cinesi finanziati dal loro governo prendono di mira sia bersagli militari che civili.

Secondo alcuni, la NSA dovrebbe avere l'incarico perché possiede conoscenze specializzate. Agli inizi del mese l'Ammiraglio Dennis Blair, direttore dell'Intelligence Nazionale, ha sostenuto proprio questo, dicendo: "Vi sono dei maghi là a Fort Meade che hanno le capacità di fare certe cose". Probabilmente non è vero, ma se lo fosse sarebbe meglio far uscire quei maghi da Fort Meade il più presto possibile -- non sono di grande aiuto al paese lì dove si trovano.

Non che le mancanze della sicurezza cibernetica governativa richiedano chissà quali magie specialistiche per porvi rimedio. I rapporti del GAO indicano che i problemi del governo comprendono controlli di accesso insufficienti, carenza di criptatura ove necessario, mediocre gestione di rete, mancanza di installazione delle patch di sicurezza, procedure di auditing inadeguate, e programmi di information security incompleti o inefficaci. Non si tratta di problematiche di sicurezza supersegrete e a livello della NSA -- sono gli stessi problemi gestionali che ogni CIO deve affrontare in ambito aziendale.

Tutti abbiamo gli stessi problemi, per cui occorre condividere le soluzioni. Se il governo ha qualche idea brillante per risolvere i propri problemi di sicurezza cibernetica, di sicuro molti di noi potrebbero trarre benefici da tali soluzioni. Se ha un'idea per migliorare la sicurezza di rete, dovrebbe renderla pubblica. La cosa migliore che il governo può fare per la sicurezza cibernetica a livello mondiale è quella di utilizzare il proprio potere d'acquisto per migliorare la sicurezza dei prodotti IT che tutti usiamo. Se il governo imponesse dei requisiti di sicurezza significativi ai suoi produttori IT, quelle aziende modificherebbero i loro prodotti in modo da rientrare nei requisiti richiesti. E quegli stessi prodotti, con una sicurezza maggiore e migliore, sarebbero disponibili per noi tutti come il nuovo standard.

Inoltre, la doppia missione della NSA -- garantire sicurezza ed effettuare una sorveglianza costante -- fa in modo che la NSA abbia un inerente conflitto di interessi per quanto concerne la sicurezza cibernetica. All'interno della NSA ciò viene definito "equities issue", ossia "questione di equità". Durante la Guerra Fredda era semplice: la NSA si servì della propria esperienza per proteggere le informazioni e le comunicazioni dell'esercito americano, e al tempo stesso intercettare le informazioni e le comunicazioni dei sovietici. Ma che cosa succede quando sia i 'buoni' (che la NSA vuole proteggere) sia i 'cattivi' (le cui comunicazioni la NSA vuole intercettare) si servono degli stessi sistemi? Entrambi utilizzano Microsoft Windows, database Oracle, la posta elettronica e Skype. Quando la NSA scopre una vulnerabilità in uno di quei sistemi, notifica il produttore e sistema la vulnerabilità, proteggendo di conseguenza sia i buoni che i cattivi? Oppure non rivela a nessuno la vulnerabilità, in modo che sia più facile

spiare i cattivi ma lasciando a rischio anche i buoni? Programmi come quello della NSA per l'intercettazione senza mandato hanno creato ulteriori vulnerabilità nelle nostre reti telefoniche nazionali.

Giorni fa, testimoniando di fronte al Congresso, Amit Yoran, ex capo della divisione per la Sicurezza Cibernetica del Dipartimento per la Sicurezza Nazionale, ha detto che "la comunità dell'intelligence ha sempre dato priorità, e sempre darà priorità al proprio lavoro di raccolta di informazioni piuttosto che alla missione di difesa e protezione dei sistemi digitali del nostro governo e del nostro paese".

Magari la NSA potrebbe convincerci che sta mettendo la sicurezza cibernetica davanti a tutto il resto, ma la sua cultura di segretezza farà in modo che qualsiasi decisione presa dalla NSA risulti sospetta. Secondo la legge attuale, estesa dalla stravagante invocazione del privilegio dei 'segreti di stato' da parte dell'amministrazione Bush a seguito dell'accusa di violazioni statutarie e costituzionali, le attività della NSA non sono soggette ad alcuna supervisione pubblica significativa. E la sua tradizione di segretezza militare rende molto difficile alla NSA coordinarsi con altri dipartimenti IT governativi, la maggior parte dei quali non possiede livelli di autorizzazione sufficienti; e men che meno coordinarsi con le forze dell'ordine locali o con il settore commerciale.

Servono procedimenti governativi trasparenti e responsabili, che utilizzino prodotti commerciali per la sicurezza. Servono programmi governativi di sicurezza cibernetica che migliorino la sicurezza per tutti. La NSA riveste certamente un ruolo consultivo e di coordinamento nell'ambito della sicurezza cibernetica nazionale, e forse un ruolo più di supervisione nell'ambito della sicurezza cibernetica del Dipartimento della Difesa (sia da un punto di vista offensivo che difensivo) -- ma non dovrebbe essere direttamente responsabile della sicurezza cibernetica del governo.

Rimandi:

<<http://www.washingtonpost.com/wp-srv/business/documents/fismachart.html>>
<<http://www.gao.gov/new.items/d08496t.pdf>>
<<http://uk.reuters.com/article/usPoliticsNews/idUKTRE5190B820090210>>
<<http://www.scmagazineus.com/House-hearing-US-in-dangerous-cybersecurity-state/article/128576/>>
<http://news.cnet.com/8301-13578_3-10191170-38.html>
<<http://blog.wired.com/defense/2009/03/breaking-cyber.html>>
<http://blog.wired.com/defense/files/ncsc_directors_resignation1.pdf>
<http://news.cnet.com/8301-13578_3-10195208-38.html>
<<http://hsdailywire.com/single.php?id=7574>>
<http://news.cnet.com/8301-13578_3-10194459-38.html>
<http://news.cnet.com/8301-13578_3-10045980-38.html>
<http://www.dni.gov/testimonies/20090225_transcript.pdf>
<<http://www.gao.gov/new.items/d08496t.pdf>>
<<http://www.gao.gov/new.items/d08525.pdf>>
<http://www.schneier.com/blog/archives/2008/05/dualuse_technol_1.html>
<http://www.washingtonpost.com/wp-dyn/content/article/2007/08/08/AR2007080801961_pf.html>
<<http://blog.wired.com/27bstroke6/2009/03/nsa-dominance-o.html>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog: <http://www.schneier.com/blog/archives/2009/04/who_should_be_i.html>

Una versione di questo articolo è apparsa sul sito Web del Wall Street Journal.
<<http://online.wsj.com/article/SB123844579753370907.html>>

** *** ***** ***** ***** ***** ***** ***** *****

News

Privacy e Google Latitude: buone notizie.
<<http://blog.wired.com/business/2009/03/googles-latitud.html>>

Lasciare bambini piccoli in auto. Può capitare, e a volte muoiono.
<http://www.schneier.com/blog/archives/2009/03/leaving_infants.html>

Un pezzo interessante di storia della crittografia: un codice ideato da Robert Patterson e inviato a Thomas Jefferson nel 1801.
<http://www.schneier.com/blog/archives/2009/03/1801_cipher_sol.html>

L'azienda chimica Bayer si rifiuta di parlare di un grave incidente accaduto a una centrale nel West Virginia, facendo riferimento a una legge antiterrorismo del 2002.
<<http://pubs.acs.org/cen/news/87/i11/8711news6.html>>
The meeting has been rescheduled. No word on how forthcoming Bayer will be.
<http://www.csb.gov/index.cfm?folder=news_releases&page=news&NEWS_ID=461>
oppure <<http://tinyurl.com/cckma9>>

Una ricerca su come prendere l'"impronta digitale" della carta:
<<http://www.freedom-to-tinker.com/blog/felten/fingerprinting-blank-paper-using-commodity-scanners>>
oppure <<http://tinyurl.com/djvdz>>
<<http://citp.princeton.edu/pub/paper09oak.pdf>>

Un'altra apparizione di Blowfish nella serie televisiva "24":
<http://www.schneier.com/blog/archives/2009/03/blowfish_on_24_1.html>

Un'analisi interessante dei motivi per cui si rubano i libri rari.
<<http://www.ft.com/cms/s/2/d41a83d6-09dc-11de-add8-0000779fd2ac.html>>

Il mese scorso ho pubblicato dei link che rimandavano a un catalogo di video-corsi della NSA del 1991. Ecco un aggiornamento, con nuove informazioni (aggiunte dopo il ricorso secondo il FOIA).
<http://www.governmentattic.org/2docs/NSA_TV_Center_Catalog_1991-Update.pdf>
oppure <<http://tinyurl.com/d2ds68>>

Incredibile ma vero: nel Regno Unito, una unità artificieri è stata chiamata perché qualcuno ha visto una riproduzione in plastica della Granata Sacra di Antiochia (dal film "Monty Python and the Holy Grail").
<http://www.schneier.com/blog/archives/2009/03/holy_hand_grena.html>

Ricerca interessante sul rilevamento degli esplosivi.
<http://www.aip.org/press_release/detecting_explosives.html>

Un articolo di Psychology Today sulla paura e l'euristica della disponibilità:

<<http://blogs.psychologytoday.com/blog/the-narcissus-in-all-us/200903/mass-murder-is-nothing-fear>>

oppure <<http://tinyurl.com/c8mkzm>>

Dal Kentucky: credo che questo sia il primo caso documentato di frode elettorale negli Stati Uniti facendo uso di macchine per il voto elettronico (vi sono parecchi casi documentati di errori e problemi nella procedura di voto, ma questo è il primo a presentare premeditazione malevola). Un resoconto ricco di dettagli, che vale la pena leggere.

<http://www.schneier.com/blog/archives/2009/03/election_fraud.html>

Intercettare i tasti battuti su una tastiera mediante un laser:

<http://news.zdnet.com/2100-9595_22-280184.html>

Per sopravvivere a un attacco di un dinamitardo suicida è molto importante il punto in cui ci si trova.

<<http://www.sciencedaily.com/releases/2009/03/090323161125.htm>>

Presumibilmente i ricercatori hanno anche scoperto il punto in cui dovrebbe posizionarsi l'aggressore per ottenere l'impatto più letale possibile, ma non vi sono indicazioni in tal senso.

Un'impressionante minaccia da trama cinematografica che riguarda il plasma solare.

<<http://www.newscientist.com/article/mg20127001.300-space-storm-alert-90-seconds-from-catastrophe.html?full=true>>

oppure <<http://tinyurl.com/c3xphd>>

Paure legate alla sicurezza spingono l'Iran ad adottare Linux:

<<http://www.theage.com.au/articles/2004/09/21/1095651288238.html>>

Un rilevatore di gorilla, dai Muppet Labs.

<<http://www.youtube.com/watch?v=4QrelL9fOjY>>

Bob Blakley fa un discorso interessante in merito a quel che definisce "la zona di rischio essenziale": "se si effettuano transazioni di media grandezza e poco frequentemente, si è nei guai. Le transazioni sono abbastanza consistenti da non rendere indifferenti le eventuali perdite, non si ha un volume di transazioni sufficiente ad ammortizzare tali perdite, e il costo dell'assicurazione o della garanzia è così alto in rapporto al valore delle transazioni che proteggersi non ha economicamente senso".

<<http://notabob.blogspot.com/2009/03/zone-of-essential-risk.html>>

Scoperta un'imponente rete di spionaggio cinese:

<http://www.schneier.com/blog/archives/2009/03/massive_chinese.html>

Furti al Museum of Bad Art (lett. Museo dell'Arte Mediocre):

<http://en.wikipedia.org/wiki/Museum_of_Bad_Art>

Fate attenzione soprattutto alla telecamera:

<<http://en.wikipedia.org/wiki/File:MOBAcamera.JPG>>

Ecco una storia su una serie di falsi positivi molto costosa. La polizia tedesca ha passato anni e speso milioni di dollari sulle tracce di un killer misterioso il cui DNA era stato trovato sulle scene di sei omicidi. Alla fine la polizia si è resa conto di star seguendo un

dipendente della fabbrica che costruiva i bastoncini preconfezionati usati per il test del DNA.

<http://scienceblogs.com/authority/2009/03/the_phantom_of_heilbronn_and_n.php>
oppure <<http://tinyurl.com/d5cwww>>

Questa storia potrebbe venire utilizzata per giustificare la creazione di un enorme database di DNA. Dopotutto, se quel dipendente avesse avuto il suo DNA registrato nel database, la polizia avrebbe ben presto scoperto la natura del problema.

Identificare le persone mediante informazioni anonime di social networking:

<http://www.schneier.com/blog/archives/2009/04/identifying_peo.html>

Cosa temere: un resoconto dettagliato delle statistiche.

<<http://www.counterpunch.org/goekler03242009.html>>

Un cripto-puzzle e problema della NSA:

<<http://www.cryptosmith.com/archives/565>>

Brillanti furti di identità nel social networking:

<http://www.schneier.com/blog/archives/2009/04/social_networkki.html>

Poteri della polizia e governo britannico negli Anni Ottanta:

<http://www.schneier.com/blog/archives/2009/04/police_powers_a.html>

Ricerca per la preservazione della privacy nell'ambito del peer-to-peer:

<<http://www.physorg.com/news158419063.html>>

Un articolo che parla (senza portare alcun esempio fattuale) di aziende straniere che hackerano la rete elettrica statunitense invita al panico. Secondo me è stato congegnato deliberatamente da qualcuno in cerca di argomenti su cui far leva in vista della prossima battaglia per il budget.

<http://www.schneier.com/blog/archives/2009/04/us_power_grid_h.html>

Un suggerimento: quando passeggiate in pubblico portando con voi dei documenti governativi segreti, metteteli in una busta. Non lasciateli in vista in luoghi dove la gente possa leggerli (e fotografarli).

<http://www.schneier.com/blog/archives/2009/04/how_not_to_carr.html>

Dettagli dell'arresto effettuato in fretta e furia dopo la divulgazione del fatto precedente:

<<http://www.timesonline.co.uk/tol/news/uk/article6078397.ece>>

È segno della nostra ritrovata sanità mentale il fatto che nessuno abbia chiamato la TSA in merito ai Tweenbots:

<<http://www.tweenbots.com/>>

Come scrivere un'allarmante storia di cyber-terrorismo. I consigli provengono nientemeno che dagli Affari Esteri.

<http://neteffect.foreignpolicy.com/posts/2009/04/11/writing_the_scariest_article_about_cyberwarfare_in_10_easy_steps>

** *** ***** ***** ***** ***** ***** ***** *****

La privacy e il Quarto Emendamento

Negli Stati Uniti, il concetto di "aspettativa di privacy" è molto importante perché è la prova costituzionale, basata sul Quarto Emendamento, che stabilisce quando e come il governo possa invadere la nostra privacy.

Basata sulla decisione della Corte Suprema del caso "Katz contro gli Stati Uniti" del 1967, questa prova è costituita in realtà da due parti. In primo luogo, l'azione del governo non può trasgredire l'aspettativa di privacy soggettiva di un individuo. In secondo luogo, quell'aspettativa di privacy deve essere riconosciuta come ragionevole dalla società in generale. Questa seconda parte non si basa su dati ricavati da sondaggi; è soprattutto un'idea normativa del livello di privacy che alla gente è concesso aspettarsi, considerando l'importanza della privacy personale da un lato e l'interesse del governo per la pubblica incolumità dall'altro.

Il problema è che nella società dell'informazione di oggi, quella prova di definizione ci lascerà presto senza alcuna privacy.

Nel caso Katz, la Corte stabilì che la polizia non poteva intercettare una chiamata telefonica senza un mandato: Katz si aspettava che le sue conversazioni telefoniche fossero private, e tale aspettativa proveniva da un equilibrio ragionevole fra privacy personale e sicurezza sociale. Considerando le intercettazioni su larga scala e senza mandato della NSA, e la continua insistenza da parte dell'amministrazione precedente sul fatto che tale sorveglianza fosse necessaria a proteggere l'America dal terrorismo, è ancora ragionevole aspettarsi che le nostre conversazioni telefoniche siano private?

Fra il programma di intercettazione Internet massiva della NSA e la pubblicità dipendente dal contesto di Gmail, c'è ancora qualcuno che davvero si aspetta che la propria email sia privata? Fra le chiamate agli ISP affinché conservino i dati degli utenti e le aziende che producono pubblicità Web dipendente dal contesto, c'è da aspettarsi che la nostra navigazione del Web sia privata? Fra il malware che infetta i computer e i governi mondiali che alle frontiere richiedono sempre più spesso di poter accedere alle informazioni contenute nei portatili, i dischi rigidi non possono definirsi propriamente privati. Io di certo non credo che i miei SMS, i miei dati telefonici, o qualunque cosa scriva su LiveJournal o Facebook (a prescindere dalle impostazioni di privacy) siano informazioni private.

Sorveglianza aerea, data mining, riconoscimento facciale automatizzato, radar ai terahertz che possono 'vedere' attraverso i muri, sorveglianza all'ingrosso, scansioni cerebrali, RFID, 'registratori vitali' che registrano ogni cosa: anche se la società conserva ancora una minima aspettativa di privacy digitale, le cose cambieranno quando queste e altre tecnologie diventeranno onnipresenti. In breve, il problema di una normativa aspettativa di privacy è che questa cambia a seconda delle minacce percepite, delle tecnologie e degli abusi su larga scala.

Evidentemente qualcosa deve cambiare se vogliamo conservare un briciolo di privacy. Tre studiosi in materia legislativa hanno scritto degli articoli di revisione di leggi che affrontano i problemi dell'applicazione del Quarto Emendamento al cyberspazio e in generale al nostro mondo mediato dai computer.

Daniel Solove (della George Washington University) che tiene un blog nel sito *Concurring Opinions*, ha cercato di catturare le complessità bizantine della privacy moderna. Egli fa notare, per esempio, che le seguenti violazioni della privacy (tutte realmente accadute) sono molto diverse fra loro: un'azienda ha come bersaglio del proprio marketing un elenco di cinque milioni di donne anziane incontinenti; un gruppo di reporter riescono a entrare con l'inganno in casa di una persona e la fotografano e filmano di nascosto; il governo si serve di un sensore termico per rilevare pattern di calore nella dimora di un individuo; un giornale riporta il nome di una persona vittima di violenza sessuale. Andando al di là di semplici definizioni, come il divulgare un segreto, Solove ha sviluppato una tassonomia della privacy e dei danni risultanti dalla violazione delle varie categorie.

Le 16 categorie enucleate da Solove sono: sorveglianza, interrogazione, aggregazione, identificazione, insicurezza, utilizzo secondario, esclusione, violazione delle norme di riservatezza, divulgazione, esposizione, aumentata accessibilità, ricatto, appropriazione, distorsione, intrusione e interferenza decisionale. L'obiettivo di Solove è quello di offrire una disamina coerente ed esaustiva di ciò che tradizionalmente è un concetto sfuggente e difficile da spiegare: le violazioni della privacy. (Questa tassonomia viene trattata anche nel libro di Solove, "Understanding Privacy").

Orin Kerr, anch'egli professore di giurisprudenza alla George Washington University, e blogger presso il sito *Volokh Conspiracy*, ha cercato di delineare dei principi generali per l'applicazione del Quarto Emendamento a Internet. Anzitutto Kerr fa notare che la distinzione tradizionale fra interno ed esterno -- la polizia può controllarci senza mandato in un luogo pubblico, ma non può farlo in casa nostra -- non funziona altrettanto bene in rapporto al cyberspazio. Egli invece propone una distinzione fra informazioni di contenuto e di non-contenuto: ovvero, per esempio, fra il corpo di un messaggio email e i dati degli header di quel messaggio. La polizia dovrebbe procurarsi un mandato per controllare il primo, ma non sarebbe necessario per controllare i secondi. In secondo luogo, Kerr propone che i mandati di perquisizione debbano essere scritti per determinati individui e non per determinati account internet.

Nel frattempo Jed Rubenfeld della Yale Law School ha tentato di reinterpretare il Quarto Emendamento non in termini di privacy, ma di sicurezza. Affermando che l'intera prova delle "aspettative" è circolare -- quel che fa il governo influenza ciò che il governo può fare -- Rubenfeld ridefinisce tutto in termini di sicurezza: la sicurezza che i nostri affari privati siano effettivamente privati.

Questa sicurezza viene violata quando, per esempio, il governo fa ampio uso di informatori o effettua intercettazioni su larga scala -- anche se non viene violata la privacy di nessuno. Ciò aggira efficacemente l'intera questione della privacy individuale di contro alla sicurezza sociale (un confronto dal quale l'individuo esce spesso perdente), inscrivendo entrambi gli ambiti in termini di sicurezza personale.

Personalmente, tutti e tre gli articoli presentano elementi problematici. La tassonomia di Solove è eccellente, ma il senso di indignazione che accompagna una violazione della privacy -- "Come hanno potuto sapere / fare / dire tutto ciò?" -- è una parte importante dei danni causati da una violazione della privacy. Le informazioni di non-contenuto che Kerr ritiene si possano raccogliere senza mandato, possono essere in realtà molto private e personali: gli URL possono essere molto personali, ed è possibile scoprire i contenuti di siti visitati semplicemente dalle dimensioni del traffico SSL criptato. Inoltre, la facilità con cui il governo può raccogliere tutte le informazioni di questo tipo -- il

chiamante e chi riceve la chiamata di ogni telefonata nazionale -- rende l'equilibrio molto diverso. Io ritengo che tutti questi dati debbano venire protetti dall'obbligo di un mandato. La ridefinizione di Rubenfeld è interessante, ma il diavolo è nei dettagli. Ridefinire la privacy in termini di sicurezza ha comunque come risultato un bilanciamento di diritti in competizione fra loro. Preferisco l'approccio di dichiarare l'ovvio (almeno per me) valore individuale e societario della privacy, e dare alla privacy la sua legittima parte quale diritto umano fondamentale. (Su ArsTechnica vi sono ulteriori commenti alla tesi di Rubenfeld).

Il punto è comprendere che una definizione normativa dell'aspettativa di privacy non deve necessariamente dipendere da minacce o dalla tecnologia, ma da quel che noi, come società, decidiamo che sia. Certo, le tecnologie attuali permettono di violare la privacy con una facilità mai vista. Ma da questo non segue necessariamente che si debba violare la privacy. Le armi da fuoco oggi in uso permettono di sparare praticamente a chiunque per un motivo qualsiasi. Questo non significa che le nostre leggi debbano cambiare.

Nessuno sa come tale questione sarà risolta sul piano legislativo. Questi tre articoli provengono tutti da professori di legge; non sono opinioni giudiziarie. Ma chiaramente qualcosa deve cambiare, e idee come queste potrebbero un giorno formare la base di nuove decisioni della Corte Suprema che porteranno finalmente delle nozioni legali sulla privacy nel XXI secolo.

Rimandi:

<http://www.schneier.com/blog/archives/2008/05/crossing_border.html>
<<http://www.schneier.com/essay-147.html>>
<<http://www.schneier.com/essay-261.html>>
<<http://concurringopinions.com/>>
<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622>
<http://www.concurringopinions.com/archives/2006/03/a_taxonomy_of_p.html>
<<http://www.amazon.com/Understanding-Privacy-Daniel-J-Solove/dp/0674027728>>
<<http://volokh.com/>>
<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1348322>
<<http://lawreview.stanford.edu/content/vol61/issue1/Rubenfeld.pdf>>
<<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.1201>>
<<http://www.schneier.com/essay-114.html>>
<<http://arstechnica.com/tech-policy/news/2009/03/from-the-academy-the-end-of-privacy.ars>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:
<http://www.schneier.com/blog/archives/2009/03/privacy_and_the_1.html>

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2009/03/securitymatters_0326>
oppure <<http://tinyurl.com/dh3xg5>>

** *** ***** ***** ***** ***** ***** ***** ***** *****

Le news su Schneier

Sono stato intervistato alla Federal News Radio sulle minacce costituite dagli insider:
<<http://www.federalnewsradio.com/index.php?nid=56&sid=1632741>>

Interverrò al Taiwan Information Security Center il 17 aprile a Taipei:
<<http://forum.twisc.ncku.edu.tw/dm.html>>

Farò parte della tavola rotonda dei crittografi (Cryptographers' Panel) alla RSA Conference il 21 aprile a San Francisco:
<<http://www.rsaconference.com/2009/US/Home.aspx>>

Terrò il discorso introduttivo all'IPSI Research Symposium il 6 maggio a Toronto:
<http://www.ipsi.utoronto.ca/events/IPSI_Research_Symposium_2009.htm>

Interverrò all'International Workshop on Coding and Cryptography il 12 maggio a Lofthus, in Norvegia:
<<http://www.selmer.uib.no/WCC2009/callWCC2009.pdf>>

Terrò il discorso introduttivo al secondo giorno della European OWASP Application Security Conference, il 14 maggio a Krakow, in Polonia:
<<http://www.owasp.org/index.php/AppSecEU09>>

E terrò il discorso introduttivo alla CONFidence il 15 maggio, sempre a Krakow, in Polonia:
<<http://2009.confidence.org.pl/>>

** *** ***** ***** ***** ***** ***** ***** *****

La definizione di "Armi di distruzione di massa"

Almeno, secondo la legge degli Stati Uniti:

18 U.S.C. 2332a

(2) Il termine "arma di distruzione di massa" significa --

(A) un qualsiasi ordigno distruttivo secondo quanto definito nella sezione 921 del presente testo;

(B) una qualsiasi arma progettata o destinata a provocare la morte o gravi lesioni corporali mediante il rilascio, la disseminazione o l'impatto di sostanze chimiche tossiche o velenose, o di loro precursori;

(C) una qualsiasi arma che implichi un agente biologico, una tossina o un vettore (per la definizione di tali termini si veda la sezione 178 del presente testo); oppure

(D) una qualsiasi arma progettata per emettere radiazioni o radioattività a livelli nocivi alla vita umana;

18 U.S.C. 921

(4) Il termine "ordigno distruttivo" significa --

(A) un qualsiasi esplosivo, incendiario o gas velenoso --

(i) bomba,

(ii) granata,

(iii) razzo dotato di una carica di propellente superiore a quattro once (circa 120 cc),
(iv) missile dotato di una carica esplosiva o incendiaria superiore a un quarto di oncia (circa 7,1 gr),
(v) mina, oppure
(vi) un ordigno simile a uno qualsiasi degli ordigni descritti nei precedenti paragrafi;

(B) un qualsiasi genere di arma (diversa da un fucile o da una cartuccia di fucile, che il Ministro di Giustizia considera generalmente riconosciuti come particolarmente adatti ad attività sportive) conosciuto sotto qualsivoglia appellativo che possa -- o che sia facilmente modificabile per -- espellere un proiettile mediante l'azione di un esplosivo o altro propellente, e che sia dotata di una canna con un foro di diametro superiore a mezzo pollice (1,27 cm); e

(C) una qualsiasi combinazione di parti progettate o destinate alla conversione di un dispositivo in uno qualsiasi degli ordigni distruttivi descritti nei sottoparagrafi (A) o (B), e dalla quale combinazione sia possibile assemblare prontamente un ordigno distruttivo.

Il termine "ordigno distruttivo" non comprende alcun dispositivo che non sia progettato o riprogettato per l'uso come arma; qualsiasi dispositivo, seppur originariamente concepito per essere utilizzato come arma, che venga riprogettato per un uso segnaletico, pirotecnico, demarcativo, di sicurezza, o simili dispositivi; materiale militare in surplus venduto, prestato o ceduto dal Segretario dell'Esercito secondo i provvedimenti delle sezioni 4684 (2), 4685 o 4686 del titolo 10; o un qualsiasi altro dispositivo per il quale il Ministro di Giustizia ritenga improbabile un uso come arma, o sia un oggetto di antiquariato, o sia un fucile che il proprietario intenda utilizzare unicamente a scopo sportivo, ricreativo o culturale.

Si tratta di una definizione molto generale, che comporta l'intenzione di chi ha creato l'ordigno, così come i dettagli dell'ordigno stesso.

In un'email, John Mueller (professore alla Ohio State University) mi ha scritto:

"Per come la vedo io, non solo una granata è un'arma di distruzione di massa, ma lo è anche un razzo giocattolo progettato con intenti malevoli seppur privo di testata. D'altro canto, malgrado un mortaretto spinto da un missile potrebbe essere considerato un'arma di distruzione di massa se chi lo ha progettato avesse voluto intenderlo come arma, non sarebbe considerato tale se fosse stato precedentemente ideato per essere utilizzato come arma e poi riprogettato per un uso pirotecnico, o se si tratti di surplus militare e vi sia stato venduto, prestato o ceduto (secondo determinate condizioni) dal Segretario dell'Esercito.

"Significa anche che ci stiamo avvicinando al 25esimo anniversario del patto segreto dell'amministrazione Reagan per fornire armi (a questo punto, impropriamente definite) di distruzione di massa all'Iran in cambio degli ostaggi americani.

"Brutte notizie per lei, però. Dovrà correggere quel passaggio che a lei piace usare nelle sue presentazioni, in cui dice che tutte le armi di distruzione di massa della storia hanno ucciso meno persone della guerra in Iraq, dato che ogni tipo di artiglieria, e virtualmente ogni tipo di arma lunga militare a carica frontale se è per questo, si può considerare legalmente un'arma di distruzione di massa. Il che, tra l'altro, rende il bombardamento di Fort Sumter ancora più sinistro. Per non parlare della rivelazione

che lo Star Spangled Banner (l'inno americano) è in effetti il resoconto di un attacco con armi di distruzione di massa sulle coste americane".

Divertente, senza dubbio, ma vi è un aspetto importante da considerare. Il governo degli Stati Uniti ha passato determinate leggi sulle "armi di distruzione di massa" perché sono particolarmente spaventose e dannose. Ma generalizzando la definizione di armi di distruzione di massa, chi scrive le leggi estende di gran lunga la loro applicabilità. E mi chiedo quanti fra coloro che votano a favore di tali leggi si rendano conto della loro effettiva genericità o, se davvero se ne rendono conto, se votino a favore di quelle leggi in ogni caso perché non possono o non vogliono sembrare 'tolleranti' in fatto di armi di distruzione di massa.

Ciò mi fa ricordare quei provvedimenti del PATRIOT Act statunitense -- e altre leggi -- che hanno creato i poteri di polizia affinché vengano impiegati per la lotta "al terrorismo e ad altri crimini".

Processi basati su questa definizione irragionevole:

<<http://www.ph2dot1.com/2008/04/wmd-arent-what-they-used-to-be.html>>

** *** ***** ***** ***** ***** ***** ***** *****

I furti di materiali di prima necessità

Prima di essere arrestato, Tom Berge rubava coppi di piombo dai tetti di svariati edifici nel sud-est dell'Inghilterra, fra cui lo Honeywood Museum di Carshalton, la chiesa parrocchiale di Croydon, e il liceo femminile di Sutton. Rivendeva poi quei coppi a chi ricicla scarti metallici.

In qualità di esperto di sicurezza, trovo questa storia interessante per due ragioni. In primo luogo, fra tutti i tentativi sempre più ridicoli di vietare o quantomeno censurare Google Earth per paura che possa aiutare i terroristi, ecco un reato che si affidava davvero su questo servizio: Berge utilizzava Google Earth per effettuare le sue ricognizioni.

Ma ancor più interessante è la discrepanza fra il valore dei coppi di piombo per il proprietario originale e per il ladro. La scuola di Sutton ha dovuto spendere 10.000 sterline per comprare nuovi coppi di piombo; la chiesa di Croydon ha dovuto effettuare tutta una serie di riparazioni dopo il furto, per i danni causati all'acqua. Ma Berge ha ricevuto soltanto 700 sterline per tonnellata dai commercianti di scarti metallici di Londra.

Non si tratta di un caso isolato; la stessa dinamica è in atto anche per altri materiali di prima necessità.

Vi è un'epidemia mondiale di furti di fili di rame; il rame viene rubato da centrali telefoniche ed elettriche, persino dai pali stradali, e i ladri hanno finito per uccidersi perché non si sono resi conto dei pericoli dell'alta tensione. La gente ritorna dalle vacanze e scopre che hanno rubato le tubature di rame dalle loro case. Nel 2001 gli scarti di rame valevano 70 cent per libbra. Nell'aprile 2008, quattro dollari.

Il furto di benzina direttamente dai veicoli è diventato più diffuso con l'innalzamento dei prezzi alle pompe. E il grasso di scarto dei ristoranti, che una volta veniva regalato o venduto agli agricoltori per un prezzo simbolico, viene ora rubato dai parcheggi dei ristoranti e trasformato in combustibili ecologici. I giornali e altro materiale riciclabile vengono rubati dai marciapiedi, e gli alberi vengono rubati e rivenduti come alberi di Natale.

Si rubano le recinzioni metalliche da edifici e case di privati, si rubano i coperchi dei tombini in mezzo alle strade, si rubano i guard-rail in alluminio dalle autostrade. Anche l'acciaio viene rubato a scopo di riciclaggio. In Ucraina, nel 2004, dei ladri riuscirono a rubare un intero ponte.

Questi reati si rivelano essere particolarmente costosi per la società poiché il costo necessario alla sostituzione del materiale rubato è molto più alto di quel che guadagna il ladro. Il coperchio di un tombino vale dai 5 ai 10 dollari come scarto metallico, ma sostituirne uno costa 500 dollari, manodopera compresa. Un ladro può ottenere scarti di rame per un valore di 20 dollari da un cantiere, ma il suo furto provoca 10.000 dollari di danni. E anche se i ladri non riescono a impadronirsi del rame o dell'acciaio, la minaccia sempre più diffusa induce a spendere ancor più denaro in misure di sicurezza per proteggere quei materiali di prima necessità.

Possiamo considerare la sicurezza come una tassa sugli onesti, e questi furti dimostrano che le nostre tasse sono in aumento. E a differenza di tante altre tasse, non ricaviamo alcun beneficio dalla loro raccolta. Per la società, il costo di aggiungere dei lucchetti ai coperchi dei tombini, o di sostituirli con alternative meno 'rivendibili', è molto alto; ma l'unico beneficio che si riceve in cambio è la riduzione dei furti.

Questi reati sono un segnale del futuro: pressione evolutiva sulla nostra società, se vogliamo. Spesso i criminali vengono definiti come parassiti sociali: si attaccano alla società, dissanguandola, ma non offrono alcun beneficio utile. Sono però una specie di sistema d'allarme che segnala in anticipo le trasformazioni societarie. Liberi da leggi o restrizioni morali, i criminali possono essere i primi a rispondere a quei cambiamenti che il resto della società affronterà con maggiore lentezza. Infatti è in atto una tregua: i prezzi dei metalli di scarto sono tutti in discesa rispetto all'anno scorso. Il rame è valutato 1,62 dollari a libbra attualmente, e il piombo alla metà di quanto ha ottenuto Tom Berge. Di conseguenza anche i furti stanno diminuendo.

Abbiamo progettato gran parte della nostra infrastruttura dando per scontato che i materiali di prima necessità costino poco e che i furti avvengano di rado. Non proteggiamo le linee di comunicazione, i coperchi dei tombini, le recinzioni metalliche o i rivestimenti in piombo sui tetti. Ma se i prezzi di questi materiali sono destinati ad aumentare, la società finirà con il reagire e troverà soluzioni alternative a tali materiali, oppure troverà dei modi per proteggerli. I criminali sono stati i primi a evidenziare questo aspetto, e continueranno a sfruttare il sistema finché questo si stabilizzerà nuovamente.

Rimandi:

<<http://www.telegraph.co.uk/news/uknews/4995293/Google-Earth-used-by-thief-to-pinpoint-buildings-with-valuable-lead-roofs.html>>

<<http://www.independent.co.uk/news/uk/crime/thief-googled-163100000-lead-roofs-1645734.html>>

<<http://www.hindu.com/yw/2009/03/17/stories/2009031750530300.htm>>

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=networking_and_internet&articleId=9121819&taxonomyId=16&intsrc=kc_to_p>
<http://news.cnet.com/8301-10787_3-10193237-60.html>
<<http://www.cnn.com/2009/TECH/03/11/google.earth.censor.california/index.html>>
<<http://www.guardian.co.uk/technology/2009/jan/29/read-me-first-google-earth>>
<<http://www.telegraph.co.uk/comment/3554019/Pillar-boxes-could-be-next-to-go-missing.html>>
<http://www.csoonline.com/article/221225/Red_Gold_Rush_The_Copper_Theft_Epidemic/1>
<http://www.ajc.com/metro/content/metro/stories/2008/05/13/CopperTheft_Death.html>
<http://www.news8austin.com/content/top_stories/default.asp?ArID=201560>
<http://www.onlineathens.com/stories/062908/news_20080629063.shtml>
<<http://www.click2houston.com/news/4418348/detail.html>>
<http://www.fosters.com/apps/pbcs.dll/article?AID=/20080626/GJNEWS_01/23528739/-1/FOSNEWS>
<http://www.cbs47.tv/news/local/story.aspx?content_id=be988a92-ff69-4701-a6b0-d95fd1634efc>
<<http://www.msnbc.msn.com/id/24729484/>>
<<http://www.csmonitor.com/2008/0506/p01s03-usgn.html>>
<<http://query.nytimes.com/gst/fullpage.html?res=990CEEDC1038F930A3575AC0A963958260&fta=y>>
<<http://www.nytimes.com/2007/10/15/nyregion/15recycle.html>>
<<http://query.nytimes.com/gst/fullpage.html?res=9D0CE0D71338F936A25751C1A967958260&fta=y%E2%80%9D%3Etrees>>
<<http://cbs13.com/local/sacramento.home.fence.2.849307.html>>
<http://www.nytimes.com/2008/07/23/us/23manholes.html?_r=1>
<<http://query.nytimes.com/gst/fullpage.html?res=9404E2DB1F3DF935A35756C0A9629C8B63&fta=y>>
<<http://cominganarchy.com/2006/12/08/stealing-steel/>>
<<http://news.bbc.co.uk/1/hi/world/europe/3514061.stm>>
<<http://www.newsweek.com/id/137822>>
<http://www.dailybulletin.com/news/ci_4021500>
<<http://www.newsobserver.com/business/story/1438867.html>>
<http://www.syracuse.com/news/index.ssf/2009/03/scrap_metal_prices_crash_as_ec.html>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:
<http://www.schneier.com/blog/archives/2009/04/stealing_commod.html>

Una versione di questo articolo è originariamente apparsa nel Guardian:
<<http://www.guardian.co.uk/technology/2009/apr/02/google-earth-censorship-crime-comodities>>
oppure <<http://tinyurl.com/coo59n>>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

** *** ***** ***** ***** ***** ***** ***** *****

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo

<<http://www.schneier.com/crypto-gram.html>>. Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

La versione italiana è curata da Communication Valley SpA

<<http://www.communicationvalley.it/>>

Per iscriversi o cancellarsi andare all'indirizzo <<http://www.cryptogram.it/>>

I numeri arretrati sono disponibili all'indirizzo <<http://www.cryptogram.it/>>

Per informazioni <crypto-gram@communicationvalley.it>

I commenti a CRYPTO-GRAM devono essere inviati a schneier@counterpane.com. Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di BT Counterpane e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Frequentemente scrive e partecipa a conferenze sulla sicurezza informatica e sulla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

BT Counterpane è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. BT Counterpane protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

<<http://www.counterpane.com>>

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di BT o di BT Counterpane.

Copyright (c) 2009 - Bruce Schneier.